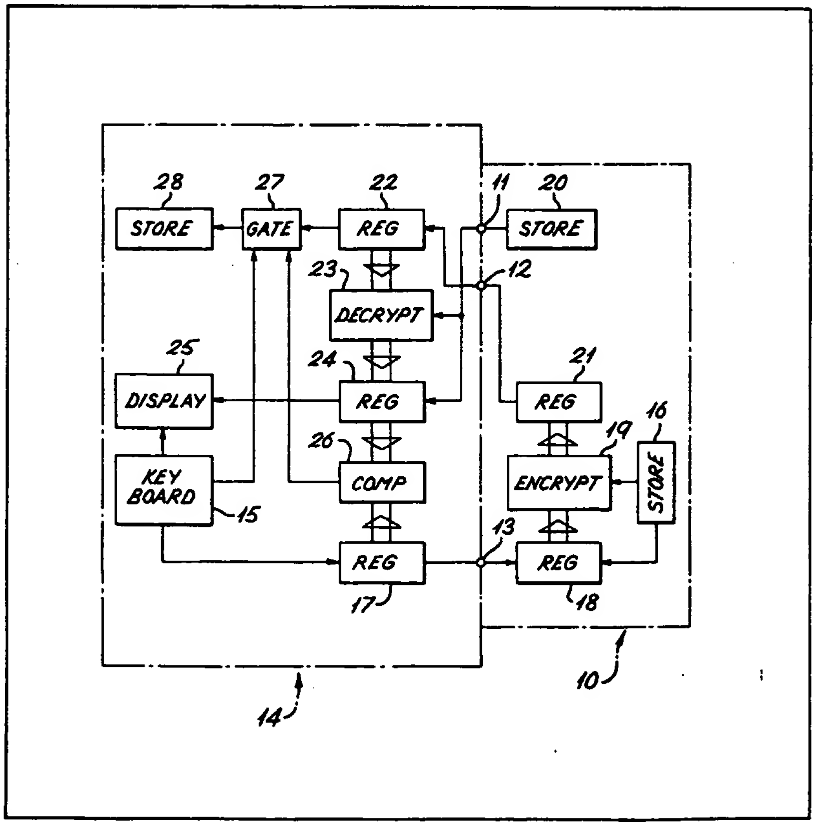
(12) UK Patent Application (19) GB (11) 2 102 606 A

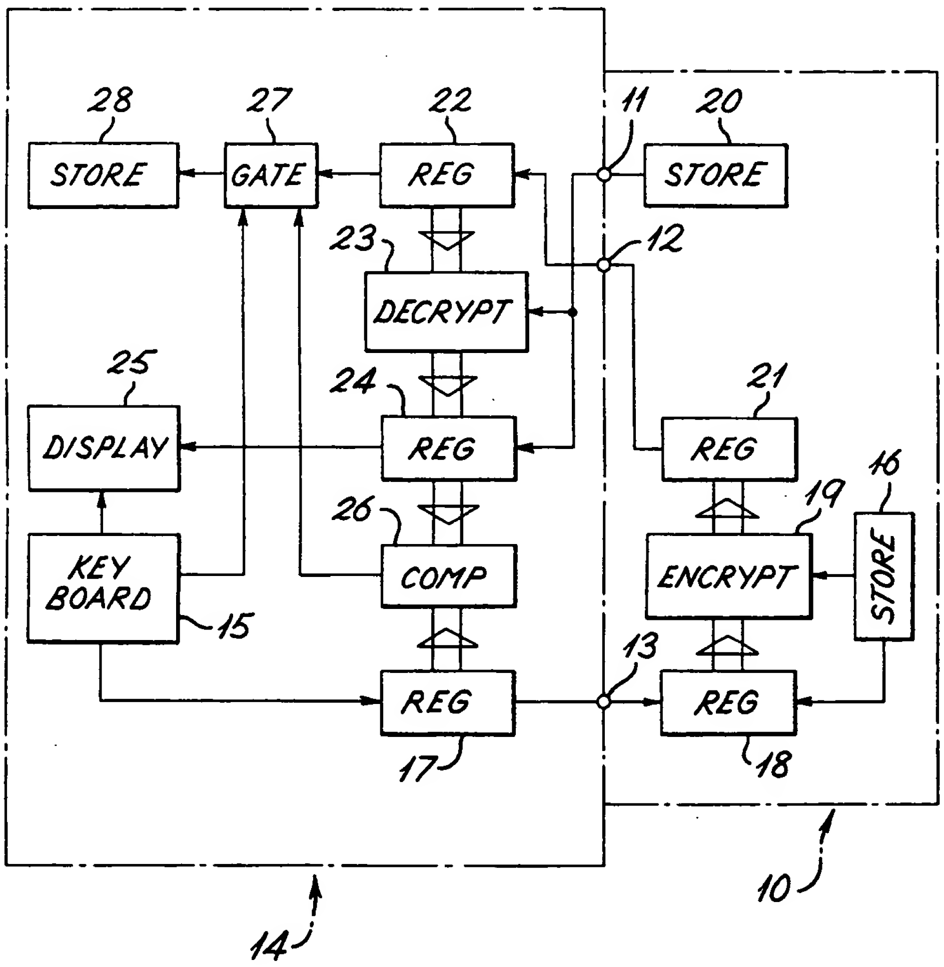
(21) Application No 8217552
(22) Date of filing 17 Jun 1982
(30) Priority date
(31) 8118942
(32) 19 Jun 1981
(33) United Kingdom (GB)
(43) Application published
2 Feb 1983
(51) INT CL³
G07F 7/10
(52) Domestic classification
G4H 13D 14A 1A TG
(56) Documents cited
None
(58) Field of search
G4H
G4A

(71) Applicants
National Research
Development
Corporation,
(Great Britain),
Kingsgate House,
66-74 Victoria Street,
London SW1E 6SL
(72) Inventor
Donald Atkinson Bell
(74) Agents
National Research
Development
Corporation,
(C. Hasler),
Patent Department,
P.O. Box 236,
66-74 Victoria Street,
London SW1E 6SL

(54) **Apparatus and methods for making payments electronically**

(57) Where simply the giving of a number is to be used as a payment, problems arise as to how the number can be generated securely and how it can be verified. A secret key held in a store 16 of a customers token 10 is used to encrypt a number specifying goods and a payment to be made transmitted from a shopkeepers terminal 14. The number generated is decrypted for checking by the terminal 14 using a non-secret key supplied by a store 20 of the token 10 but the non-secret key together with coded numbers does not provided enough information for the secret key to be found and hence for fraudulent coding to be carried out.




28
STORE
27
GATE
22
REG
11
20
STORE
12
23
DECRYPT
25
24
DISPLAY
REG
21
REG
26
16
19
COMP
ENCRYPT
STORE
KEY BOARD
15
13
REG
REG
17
18
10
14

SPECIFICATION

Apparatus and methods for making payments electronically

The present invention relates to devices such as cards or tokens containing "active" electronic circuits, and methods of using such devices for carrying out transactions, for example payments. Usually the transactions are carried out "off line".

In the most commonly used method of making payment by passive credit card, a shopkeeper, for example, fills in a slip using details from the credit card and the customer signs the slip. Where the amount is greater than a certain limit, the shopkeeper telephones the credit card company and obtains a number to write on the slip provided the customer has sufficient credit to cover the purchase. The slips are made out by shopkeepers are then passed to credit card companies who arrange for payment to the shopkeepers. Although this process works well, it is expensive and time consuming in writing out slips, and in the transmission and clearing of slips.

In another less well known credit card system which may be active or passive the customer prepays for some service such as a train fare and the amount he pays is recorded on the card. Each time the card is used an amount, for example corresponding to the fare, is deducted from the total on the card and the card has to be either discarded or reloaded when the prepaid amount has been used. Although this system is suitable for such payments as travel by railway and telephone usage, where a customer deals mainly with one organisation which can issue cards to be used only on its system, it is of little use where a card is required which can be used with a large number of relatively small organisations. Although in theory the system could be operated by transferring an amount from the customer's card to an electronic or magnetic record kept by the shopkeeper, such a system would be very susceptible to fraud.

In another proposed arrangement which is quite similar to that previously described, the shopkeeper has an electronic cash register (ECR) which is connected "on line" to a number of banks and when the credit card is used, it is inserted into the ECR and an on line computer checks the card holder's current balance and debits it according to an amount entered at the ECR. At the same time the shopkeeper's account is increased by that amount. Clearly this is a complex and expensive system which is susceptible to electronic faults.

According to a first aspect of the present invention there is provided a method of carrying out a transaction comprising automatically coding information relating to the transaction using a system of the type hereinafter specified, decoding the coded message in order to determine what information has been coded, and using the coded message to enable an action to be carried out and/or storing the coded message as evidence of the transaction.

In this specification a coding system of the type specified is a system in which a coded message can be decoded without such knowledge of the coding process which was used to produce the coded message, as would allow information to be coded according to the process.

Such a system can be based on the United States Public Key Crypto System (PKCS). This system is discussed in more detail later.

Transactions which may be carried out using the first aspect of the invention include many recording and/or authorization processes, for example authorization for, and recording of, the removal of goods, the coded message being kept by the person parting with the goods as evidence of authorization. Of course, transactions according to the first aspect of the invention include payments when the coded message is evidence of the payment and may, in effect, be regarded as the payment.

According to a second aspect of the present invention there is provided a portable token comprising means for receiving signals representing information concerning a transaction, means for encoding the signals received according to a coding system of the type hereinbefore specified, and means for providing an indication of the encoded signals.

Preferably the token is capable of being easily carried in one hand.

According to a third aspect of the present invention there is provided a terminal comprising means for supplying first electrical signals representative of information concerning a transaction to coding apparatus, means for receiving second encoded electrical signals representative of the first signals from coding apparatus, and means for decoding the second signals according to a coding system of the type hereinbefore specified.

The terminal may also include means for indicating the decoded contents of the second signals and/or means for checking the decoded signals against the first signals.

The terminal may also include storage means for storing a plurality of second signals in a form which can be transmitted to a clearing organisation, such as a bank. The storage means may be magnetic tape, for example in a cassette, a "floppy disc", a non-volatile electrical memory, or even a volatile electrical memory where the second signals can be transmitted, for example by means of a telephone line, at certain times of day.

A main advantage of the present invention can now be appreciated since when the method of the first aspect of the invention is used using a token according to the second aspect of the invention in conjunction with a terminal of the third aspect of the invention, a shopkeeper, for example, receives a number from a customer and this number may for instance represent the date, time and amount of a payment and in addition account numbers of both the customer and the shopkeeper. Since the number received by the shopkeeper is encoded according to a secret process he cannot encode further fraudulent numbers. On the other hand he can check that the number he is given represents the correct amount, recipient, date and time by decoding the number. Therefore the number given to the shopkeeper is a bankable commodity.

The token is usually formed by integrated circuits including programmable read only memory (PROM) which contains the encoding key, in a form which cannot be accessed, and an algorithm for encoding incoming signals. The encoding process is carried out in other circuits, which may include a microprocessor.

The terminal also includes a small computer such as a microprocessor which is able to respond to a decoding key which may be either supplied by the token or by a separate credit card which could employ either active or passive storage (such as a magnetic strip). There is no particular need for the decoding key to be kept secret since as is pointed out above, messages cannot be encoded using this key.

The terminal is expected to form part of an electrical cash register.

Tokens according to the second aspect of the invention or for use with terminals according to the third aspect of the invention may take many forms, for example they may be card shaped or key shaped. Tokens may be battery operated or supplied by way of plug-in contacts from a terminal or by way of impedance coupling to a terminal.

The PKCS and its application to this invention will now be discussed. The PKCS is described in "New Directions in Cryptography" by Diffie and Hellman, I.E.E.E. Trans. Inform. Theory 11, 22 (November 1976), also in "A Method for Obtaining Digital Signatures and Public-Key Crypto-systems", by Rivest, Shamir and Adlerman, Comm. Assoc. Comp. Mach. Vol 21, No. 2 (February 1978).

There are two kinds of PKCS available but only that known as the RSA algorithm is thought, at present, to be suitable for the present invention. The RSA is a number theoretic system which makes public two numbers R and S. If the message is M then the encrypted message C is given by:

$$C = M^S \text{ (mod R)}$$

The recipient knows a decryption key which is another number T which has the property that $M = C^T$ (mod R) and therefore he can decode C to obtain M. If R is the product of two large primes P and Q, then calculation of T, given S and R, is only possible if R can be factorised into PXQ. This is known to be very difficult for large numbers (especially if, $P = 2P' + 1$ where P' is also prime). An advantage of the RSA algorithm is its symmetry. It does not matter whether S or T is used for "encryption" or "decryption".

A simple example of the system is now given using the "secret" numbers P = 5, Q = 11 and T = 7, the "public" numbers R = 55 and S = 3. Suppose the message is the number 19 (in practice for payments the number has about 50 decimal digits (as is discussed below) and is in binary form) then

$$C = 19^3 \text{ (mod 55)}$$
$$= 6859 - (55 \times 120) = 39$$

(55 x 120 being the nearest multiple of 55 which is less than 6859). Thus the coded message is 39. On decoding,

$$M = 39^7 \text{ (mod 55)}$$

which can be found by first calculating 34^4 (mod 55) and 39^3 (mod 55) which equal 31 and 29 respectively and then finding 31 x 29 (mod 55).

That is 34 x 29 (mod 55) = 899 − 880 = 19.

An embodiment of the invention will now be described, by way of example, with reference to the accompanying drawing which is a block diagram of a customer's token and a shopkeeper's terminal according to the invention.

In the Figure a token 10, which may be in the form of a slim card, contains a number of integrated circuits and is connected by way of plug-in contacts 11, 12 and 13 to a terminal 14 which is part of an ECR only some parts of which relevant to the present invention are described here. The card 10 receives power by means of plug-in connections from the ECR but these power circuits are not shown in the Figure. The card is also synchronised to the terminal by means of connections and circuits which are not shown.

When a customer makes a purchase the shopkeeper enters details of the transaction into his ECR by means of a keyboard 15. These details, which include the amount of the transaction and the date and time of the transaction, are passed to a display 25 of the terminal.

If the customer agrees with the figures displayed, he inserts his card 10 into the terminal 14, initiating the operations now described.

The information entered on the keyboard 15 is held in a register 17 together with a number identifying the shop. This information is transferred to a register 18 in the token 10 which also receives a number from a store 16 identifying the customer, for example the number of his bank plus his account number. Thus the store 18 now holds all details of the transaction and these are passed to a PKCS encryption circuit 19 which also receives the encryption key from the store 16.

The encrypted message is then passed to a register 21 and thence to a register 22 in the terminal 14. The contents of the register 22 are applied to a PKCS decryption circuit 23 which receives the decryption key from a store 20 in the token 10. Circuits 19 and 23 may be in the form of microprocessor integrated circuits programmed according to the above mentioned paper by Rivest, Shamir and Adlerman. The decoded message thus arrives in a register 24 where it is used to drive the display 25. Since this display is available to both customer and shopkeeper, both can check that the number supplied from the register 21 to the register 22 contains correct information concerning the transaction. The display 25 may include a small printer which provides a permanent record for the customer and also, if required, for the shopkeeper.

The display may also include a character which indicates whether the message as sent from the ECR to the token 10 is the same (except for the customer's number which was added in the register 18) as that obtained after decryption in the register 24. For this purpose a comparator 26 is provided and if the comparison is correct an enabling signal is applied to a gate 27. However a further enabling signal from the keyboard 15 is required which is supplied when the shopkeeper is satisfied that the details displayed are correct. The gate 27 then opens and the coded number held by the register 22 is passed to an electrical store 28.

After a number of such transactions the store 28 contains encoded numbers which represent payments. These numbers may be, as mentioned above, held on magnetic tape so that they can be taken to a bank at the end of the day or at the end of a week. Other ways of storing and transmitting the numbers have already been mentioned.

In a typical token and terminal system the message which is coded and then stored in the store 28 may be made up as follows:—

Amount (£ or $)	5 decimal digits
Date	6 decimal digits
Time	4 decimal digits
Customer's Bank	8 decimal digits
Account number	8 decimal digits
Shop	12 decimal digits

This gives a total of 43 decimal digits and by providing 50 such digits a few spare digits are available for further information.

The stores 16 and 20 may conveniently be PROMs but steps must be taken to ensure that the encoding key from the store 16 cannot be accessed from outside the token 10 without destroying the token. For some types of transaction it may be considered preferable to employ a second token or credit card instead of the store 20, which may be kept in a different place from the token 10 to give details of the decryption key for the circuit 23 in the terminal. Details relating to the owner of the token 10 may also be held on this second card instead of in the store 16. Such a card may simply include a magnetic strip with these details and printing giving the owner's name, address and, for example, bank.

Many of the circuits shown in the token 10 and the terminal 14 may be replaced by respective microprocessors.

It will be apparent that the invention may be put into effect in many other ways that specifically described above. In particular other encryption systems may prove suitable and other layouts of both token and terminal are possible using similar or different integrated circuits.

CLAIMS

1. A method of carrying out a transaction, comprising automatically coding information relating to the transaction using a system of the type hereinbefore specified, decoding the coded message in order to determine what information has been coded, and using the coded message to enable an action to be carried out and/or storing the coded message as evidence of the transaction.

2. A portable token comprising means for receiving signals representing information concerning a transaction, means for encoding the signals received according to a coding system of the type hereinbefore specified, and means for providing an indication of the encoded signals.

3. A token according to Claim 2 which is capable of being easily carried in one hand.

4. A token according to Claim 2 or 3 including first and second storage means containing an encoding key and a decoding key, respectively, the first storage means being coupled to the means for encoding, and the second storage means having coupling means for passing the decoding key to a terminal which is to be used in conjunction with the token.

5. A terminal comprising means for supplying first electrical signals representative of information concerning a transaction to coding apparatus, means for receiving second encoded electrical signals representative of the first signals from coding apparatus, and means for decoding the second signals according to a coding system of the type hereinbefore specified.

6. A terminal according to Claim 5 including means for indicating the decoded contents of the second signals and/or means for checking the decoded second signals against the first signals.

7. A terminal according to Claim 5 or 6 including storage means for storing a plurality of the second signals in a form which allows the stored signals to be transmitted later, when required.

8. A method, token or terminal according to any preceding claim wherein coding and decoding are according to the RSA alogorithm of the United States Public Key Crypto System.

9. A method of carrying out a transaction as hereinbefore described.

10. A portable token as hereinbefore described with reference to and as shown in the accompanying drawing.

11. A terminal as hereinbefore described with reference to and as shown in the accompanying drawing.

Printed for Her Majesty's Stationery Office by The Tweeddale Press Ltd., Berwick-upon-Tweed, 1983.
Published at the Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.